North Dakota
Homeland Security
Anti-Terrorism Summary

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

Quick Links

North Dakota

Nothing Significant to Report

Regional

(Minnesota) **Minnesota man charged with $80 million bank Ponzi scheme.** A 40-year-old Lakeville man was charged August 9 in federal court in the District of Minnesota with operating a Ponzi scheme that resulted in a total estimated loss of $79.5 million for 17 lenders. The suspect was charged with one count of bank fraud and one count of filing a false income tax return in connection to this crime. The Information alleges that the suspect conducted the scheme from 2005 through March of 2009. The scheme purportedly involved overselling participation in large commercial and personal loans arranged by him through his company, First United Funding ("FUF"). The suspect's alleged scheme involved selling more than 100 percent participation in at least ten different loans arranged through FUF. In other words, he purportedly sold loan participation to banks after already selling that same participation to other banks. In each instance, the suspect failed to disclose that the total participation exceeded 100 percent of the original loan, making it impossible for the participating bank to receive the full amount of money expected. Source: http://www.loansafe.org/minnesota-man-charged-with-80-million-bank-ponzi-scheme

National

(Wyoming) **Wyo., Feds investigate device found on I-80.** State and federal authorities are trying to figure out who put a device resembling a bomb under an overpass in southwestern Wyoming. The device was found August 10 near Point of Rocks, shutting down Interstate 80 in both directions for less than an hour. It was removed and destroyed and officials say it doesn't look like it contained any explosive material. The device was spotted by a passerby and appeared to have tape around it and a wire hanging from it. It was attached to one of the vertical I-beam steel girders on the eastbound side near the girder's base. The investigation is being handled by the Wyoming Division of Criminal Investigation and the Bureau of Alcohol, Tobacco, Firearms and Explosives. Source: http://cbs4denver.com/wireapnewswy/State.feds.investigate.2.1853764.html

(Texas) **Texas gov. warns of car bombs on border.** In a letter delivered to the President August 9, the Texas governor wrote, "The Mexican cartels have recently added a new deadly weapon to their arsenal: Vehicle-Borne Improvised Explosive Devices (VBIED), which they use to attack their rivals and the police." Citing car bomb examples from recent weeks just across the Texas-Mexican border in Juarez and Ciudad Victoria, the governor received no immediate answer from the President. The governor urged federal action before Texas communities suffer the same fate. In recent years, Mexican drug cartels have threatened the safety of people living in border towns. The governor requested 1,000 Title 32 National Guard troops for Texas, in addition to other resources, and said 286 National Guard personnel along the 1,200 mile border were not enough. Federal drug enforcement

agents have told Austin officials during the last year these Mexican cartels are recruiting local gang members to push their products north into the U.S. So far, they have an increase in this practice in Austin, San Antonio and Houston. Source: http://www.kxan.com/dpp/news/national/south/texas-gov-warns-of-car-bombs-on-border-

INTERNATIONAL

Bomb wracks offices in Colombia capital, injures 9. A car packed with at least 110 pounds of explosives blew up in an office district of Colombia's capital, Bogota, August 12, shattering windows in dozens of buildings and injuring nine people. No deaths were reported. The blast occurred at 5:30 a.m. outside a 12-story building housing Caracol Radio, the Spanish news agency EFE, and the Ecuadorean consulate, as well as the offices of several banks and politicians. Investigators were not sure of the target or who was behind the bombing. The president hurried to the scene and called the explosion "a terrorist act," saying it was meant to sow fear and create skepticism about the government. Most of those hurt had been on a bus that was passing by as the bomb exploded. Authorities said no arrests had been made. Source: http://www.google.com/hostednews/ap/article/ALeqM5hB4P7UUGsLNmFp0oUyksHevzz02wD9HI7C781

India equipped to protect the October Commonwealth Games against WMD attacks. Indian security agencies say they are equipped to face chemical, biological, radiological, and nuclear (CBRN) terrorist threats during the Commonwealth Games begin in October. Intelligence agencies have been working on the possibility of attacks from Kashmiri groups like the Hizbul Mujahidden, the Pakistan-based Lashkar-e-Taiba (LeT), the Taliban from Pakistan or Afghanistan, and Al Qaeda; militant outfits of various other ideological hues are also on the police radar. Source: http://homelandsecuritynewswire.com/india-equipped-protect-october-commonwealth-games-against-wmd-attacks

Indonesia terror suspects allegedly talked about targeting embassies. An Indonesian official said suspected members of a terror cell arrested in the past week were "chatting" about targeting foreign embassies, but it is not clear whether they planned to follow through. The head of a government anti-terror desk, said he could not confirm that the group was targeting the U.S., U.K. and Australian embassies. "They were just chatting about it, but it's not confirmed," the official said. He said the five suspected terrorists were talking about targeting the embassies during police interrogations. The official confirmed one of the main targets was the national police headquarters "because they conducted surveillance and took photos of the building," he said. On Monday, an Islamic cleric was arrested for playing a key role in the establishment of a militant training camp in Indonesia's Aceh region authorities said. Source: http://www.cnn.com/2010/WORLD/asiapcf/08/11/indonesia.cleric.arrest/index.html

Russia's nuclear storage sites safe from wildfires. Russian operator RosRao said August 10 that its 17 nuclear waste storage facilities are safe from the wildfires that have been ravaging Russia in recent weeks. Some 300 people are now working around the clock to protect RosRao's nuclear waste storage facilities from wildfires, the head of the company's nuclear and radiation safety department said in a statement. The official said the wildfire nearest a storage area in the Nizhny Novgorod region was at least six km away. In Tatarstan, the minimal distance between the storage site and three

wildfires was 10 km. The fires there have now been put either under control or extinguished. In Chelyabinsk, the Urals, the distance between the local nuclear waste deposit facility and the fire was 70 km. The official said RosRao "adopts all necessary preventive measures" to assure fire safety at all of its storage facilities. Currently, he said, the situation is normal. RosRao runs 17 sites for the storage of nuclear fuel waste throughout Russia. Some 300 people are now working around the clock to protect RosRao's nuclear waste storage facilities from wildfires, the head of the company's nuclear and radiation safety department said in a statement. The official said the wildfire nearest a storage area in the Nizhny Novgorod region was at least six km away. Source: http://english.cri.cn/6966/2010/08/10/1901s587832.htm

Radical cleric Abu Bakar Bashir arrested in Indonesia. One of Indonesia's top radical Muslim clerics was arrested August 9 in Indonesia on accusations that he played an important role in terrorist training and had links to militants plotting a series of brazen attacks on the Indonesian authorities and foreigners. The cleric was arrested along with five bodyguards in West Java on accusations that he "had an active role" in setting up a militant training camp in the northern Sumatran province of Aceh. The arrest followed weeks of speculation that the police were preparing to arrest the cleric, a founder of the radical Jemaah Islamiyah movement, which has been blamed for a series of terrorist attacks, including nightclub bombings that killed 202 people in Bali in 2002. The suspects were accused of wanting to carry out bombing attacks on the National Police headquarters, the West Java police Mobile Brigade headquarters, international hotels, and "more than two" foreign embassies. Source: http://www.nytimes.com/2010/08/10/world/asia/10indo.html?_r=1

Banking and Finance Industry

Macs not vulnerable to Eleonore online banking trojan. Macs are not being infected with the Zeus botnet say M86 Security, after reports August 12 by a number of news sources that Macs, PlayStation 3's and Nintendo Wii's had joined Windows systems as part of a banking targeted botnet. These mistaken reports of the discovery of a Zeus botnet in the UK by M86 Security had in turn lead to some security vendors calling it "the big wakeup call for Mac users." The reports of Mac infections from the M86 white paper appear to have been due to a table on page 4 of the report which lists the operating systems of machines which had connected to a web site used by the botnet's creators to spread the infection. The criminals used the Eleonore exploit kit which makes use of vulnerabilities in Internet Explorer, Adobe Reader, Java Development Kit and Java Web Start. The product manager at M86 Security confirmed to The H that the list is only of OS connection numbers and does not indicate that there had been successful exploits of the listed operating systems; the list also includes Linux, Symbian, SunOS and Windows ME. "We've only seen these exploits on Windows machines" he said, adding "The table was included in the white paper to show the sophistication of the botnet's data gathering and that it was analyzing the traffic." Source: http://www.h-online.com/security/news/item/Macs-not-vulnerable-to-Eleonore-online-banking-trojan-1057559.html

(Illinois) **Joliet bank robber claimed to have bomb.** A man claiming to have a bomb robbed a bank in southwest suburban Joliet on the morning of August 11. The deputy police chief said it was just before 10 a.m. when the bandit walked into First Community Bank, 2801 Black Road, and approached a teller. "He gave the teller a note that said he had a bomb and demanded cash," the deputy police chief said. "He then took the money and note and fled on foot." No one was injured. Source:

http://www.myfoxchicago.com/dpp/news/metro/joliet-bank-robber-claimed-to-have-bomb-20100811

(New York) **Potsdam bomb call shuts two bank sites.** A bomb threat August 11 closed for several hours the Community Bank branches on Market Street and the drive-through on May Road in Potsdam, New York. The police chief said a man called the police station at 10:02 a.m. reporting the bomb threat. The call, which came up as a restricted number, lasted 21 seconds. "The man stated there's a bomb in one of our banks," the police chief said. "We asked him which one, and he clarified 'one of your Community Banks." The Market Street parking lot surrounding the bank was closed and a police car sat near the bank's main entrance for several hours. An officer sitting in the police car was informing people of the emergency closing. Bank employees had evacuated the building, but the lights remained on inside. Employees at the Potsdam Insurance Agency and St. Lawrence County Probation Department office, in the same plaza at 70 Market St., also were evacuated. A state police K-9 unit searched each location and found no device. The Market Street location was reopened shortly before 2 p.m. Source: http://www.watertowndailytimes.com/article/20100812/NEWS05/308129974

Zeus botnet raid on UK bank accounts under the spotlight. More details have emerged of how security researchers tracked down a Zeus-based botnet that raided more than $1m from 3,000 compromised UK online banking accounts. The vice president of technical strategy for M86 Security said hackers began the assault by loading compromised third-party sites with a battery of exploits designed to infect visiting PCs with variants of the Zeus banking Trojan. Phase one of the attack used the Eleonore Exploit Kit and the Phoenix Exploit Kit to load Zeus onto compromised machines through a battery of browser and application-based vulnerabilities and drive-by download attacks. The main attack revolved around the use of version 3 of Zeus to steal money from online bank accounts. The use of a different strain of Zeus means the M86 researchers are sure the attack is unrelated to an otherwise similar attack involving 100,000 compromised UK bank accounts that was the subject of an alert by transaction security firm Trusteer the week of August 2. After noticing a pattern of possible attack, M86 researchers deliberately infected a machine in order to identify a command and control server associated with the botnet which was hosted in Moldova. They then used exploits to break into the poorly-secured system where they found logs recording the activity of compromised bank accounts. It also found that the exploit pack used to seed to attack had claimed a much larger number of victims — as many as 300,000 machines. The vast majority were Windows boxes, but 4,000 Mac machines were also hit. The logs also revealed that 3,000 online banking accounts had been victimized between July 5 and August 4. Source: http://www.theregister.co.uk/2010/08/11/zeus_cyberscam_analysis/

Corrupt repair engineer jailed for bank fraud attempt. A corrupt laptop repair engineer has gone to jail for nine months after he was convicted of hacking into the laptop of one of his customers. The 30-year-old suspect was caught browsing through pictures in a private folder and attempting to hack into an online banking account during a Sky News investigation into computer repair services. As part of the investigation a laptop with a simple fault, rigged to ensure that its webcam covertly filmed "repairs", was deposited at Laptop Revival in Hammersmith. He used his access to the machine to attempt to access Facebook, eBay and online banking accounts using a "password file" left on the machine. A total of six attempts were made to access the online banking account, Sky News reports. Sky News passed on the results of its investigation to the Met Police, who subsequently charged the

suspect with attempted fraud. Source: http://www.theregister.co.uk/2010/08/09/corrupt_comp_repair_tech_jailed/

Chemical and Hazardous Materials Sector

(New York) **N.Y. nuclear risk assessment described.** U.S. researchers have announced an improved method of predicting where people might be exposed to radiation from nuclear waste disposal sites. Engineering and scientific experts associated with U.S. and New York state energy agencies focused on a buried nuclear waste disposal facility at West Valley, New York, a Society for Risk Analysis release said August 11. Researchers say their study looked at possible scenarios, likelihoods and consequences of a threat to the disposal site and concluded "a release resulting in a dose of 100 millirems in one year, or more, is extremely unlikely during the next 30 years of operation of the state managed disposal area at the Western New York Nuclear Service Center." By comparison, the study said, the public is exposed to approximately 300 millirems a year of cosmic radiation in the atmosphere with no visible health effects. Possible scenarios were considered involving hypothetical releases of radionuclides by liquid, solid or air pathways. The scientific analysis supports a decision to continue management of waste at the site for another decade, the researchers said. Source: http://www.upi.com/Science_News/2010/08/12/NY-nuclear-risk-assessment-described/UPI-72831281648110/

(Vermont) **Eight arrested at VY.** Eight women were arrested in front of the Vermont Yankee nuclear power plant August 10 for unlawfully trespassing on the site while protesting its continued operations. Holding a banner reading "No More Leaks & Lies! Shut it Down Now," the eight women pulled into the nuclear plant's front parking area shortly after 3 p.m. and walked into the gated entrance, a restricted zone where many of the Shut It Down Affinity Group protesters have demonstrated in previous years. This is the ninth time the group has protested on the nuclear plant's property. While sitting at the gates of Vermont Yankee, the protesters read aloud from a prepared statement saying they have exhausted all other means to close the 38-year-old plant. They used the August 10th events to call for a thorough investigation of the U.S. Nuclear Regulatory Commission as well. Source: http://www.reformer.com/ci_15737380?source=most_viewed

(Pennsylvania) **State offering anti-radiation pills for those near nuke plants.** York County residents living near nuclear power plants can receive free potassium iodide tablets from the Pennsylvania Department of Health. The tablets will be available between 3 and 7 p.m. Thursday, August 12, at these sites: Airville Fire Co., 3576 Delta Road, Airville. Fishing Creek Salem United Methodist Church, 402 Valley Road, Etters. York County State Health Center, 1750 N. George St., Manchester Township. For information, call the Pennsylvania Department of Health at 1-877-724-3258, or visit its Web site at www.health.state.pa.us. Source: http://www.yorkdispatch.com/news/ci_15701599

Commercial Facilities

(New Hampshire) **Park evacuated due to homemade pipe bomb.** Emergency responders evacuated Watson Park on Tuesday afternoon after an off-duty police officer found what appeared to be a homemade pipe bomb near the junction of the Merrimack and Souhegan rivers. Merrimack and Nashua police officers responded to the park, across from the town's central fire station on the

Daniel Webster Highway, about 1:15 p.m. after an off-duty Nashua officer noticed the bomb in the water near the river bank, according to a Merrimack police Sargent. The bomb, made of a cast iron material, had been in the water for some time and posed little risk to the public. Officers asked park visitors to vacate the area while the Nashua Police Bomb Squad secured the explosive. They reopened the park without incident after about two hours, according to a Nashua Police sergeant who is a bomb squad supervisor. Source: http://www.nashuatelegraph.com/news/820094-196/merrimack-park-evacuated-due-to-homemade-pipe.html

(Georgia) **Soldiers accused of throwing explosives at crowd could face military charges, too.** Three north Georgia soldiers accused of throwing military explosives at a crowd gathered in a Dawsonville grocery store parking lot face numerous criminal charges, including domestic terrorism, possession of an explosive device, 16 counts of aggravated assault, and two counts of first degree cruelty to children. They were based at Camp Frank D. Merrill near Dahlonega. Army investigators are standing by to help the Dawson County Sheriff investigate the case against the soldiers, said an Army spokesman from Fort Benning. The enlisted men allegedly tossed two weapon simulators at the crowd. They contain no shrapnel, yet they are incendiary and they pack an explosive punch that could cause injury, according to military experts. A Dawson County Sheriff's lieutenant told the AJC that 911 operators received a call August 8 around 1:30 a.m. about two pipe bombs tossed from a Cadillac with three occupants at a Dawsonville parking lot. The Cadillac fled up Georgia 400, and deputies who heard the explosions caught up to them. The deputies found a dozen undetonated devices that had been thrown from the car. Police have not released a motive in the case, but the executive officer at Camp Merrill said, "Alcohol was involved." Source: http://www.ajc.com/news/soldiers-accused-of-throwing-589283.html

(Washington) **Bomb damages car in Warden.** A car was damaged by a bomb the night of August 7 while parked at Lamb Weston/BSW in Warden. No one was injured by the blast and there was no damage to nearby vehicles or the potato processing plant, according to the public information officer for Grant County Emergency Management. Investigators determined the bomb was set off inside the car. When it exploded, it blew the windows out of the vehicle. "The sound of an explosion had been heard throughout the town, and a plant security guard reported a car had exploded in the parking lot," he said. Warden police are being assisted in their investigation by the Bureau of Alcohol, Tobacco, Firearms and Explosives and the Grant County Sheriff's Office. "To protect the integrity of the investigation, this is the only information which will be publicly released. Further information will likely be released at a later date," the public information officer stated. Source: http://www.columbiabasinherald.com/news/article_43521e1c-a405-11df-ba55-001cc4c002e0.html

(Florida) **Police: Teen fakes bomb in attempted robbery.** Two Lake City, Florida, teens were arrested early August 9 after they tried to rob an Exxon convenience store, Columbia County deputies said. Deputies said one of the 18-year-olds walked into the store on State Road 47 and told the clerk he had a bomb. Deputies said he showed the clerk two red sticks that were in his waistband and demanded money, saying he had a detonator in his hand. Deputies said the clerk went behind the counter and locked himself inside, telling the teen he was on video. The teen then left the store. Deputies said they found the teen's vehicle at a home on Hudson Lane. They said the suspect told a deputy he had just attempted to rob the store, and he was arrested. Another suspect told the deputy he drove his accomplice to the store so that he could rob it. The former suspect told deputies that the

robbery was the driver's idea because he was behind on rent and needed the money, deputies said. Both were arrested. Their bonds were each set at $105,000. Deputies said they were searching for the fake explosives. Source: http://www.news4jax.com/news/24564765/detail.html

(California) **W Hotel evacuated due to man making bomb threats from roof.** Guests were evacuated as a man reportedly barricaded himself on the roof the W Hotel in Hollywood, California, shouting to anyone that would hear him that he had a bomb. A man stood on the roof for several hours August 8 and made threats. Witnesses say the man was acting belligerently, claimed to have a bomb, and was uncooperative with authorities. Authorities say the man may have a mental health problem. The hotel was reportedly surrounded by squad cars and a helicopter after it was evacuated. By 6:00 p.m. the man was arrested and taken into custody by the Los Angeles Police Department, Hollywood Division, officers confirmed. The incident is under investigation. Source: http://www.ktla.com/news/landing/ktla-w-hotel-bomb-threat,0,4148606.story

(Oregon) **Suspicious device prompts evacuation of aquatic center.** Woodburn Police police say a suspicious device was placed outside a Woodburn, Oregon aquatic center. It was found before 1 p.m. August 8 by an aquatic center employee. Authorities evacuated the facility. The Oregon State Police Bomb Squad was called to the scene to examine the device, which later was determined to be non-explosive. Authorities are not releasing details about the device, citing an ongoing investigation. Source: http://www.statesmanjournal.com/article/20100809/NEWS/8090326/1001

(California) **Suspicious device at Concord park not a bomb, police say.** A suspicious device found at Newhall Park in Walnut Creek, California that prompted a bomb squad response this morning was not an explosive, police said. Someone called police about 9 a.m. to report the discovery, near one of the park's picnic areas. The Walnut Creek Police Bomb Squad, which serves the entire county, was summoned and determined that the device was not dangerous. The suspicious object was the fourth found at the park in about two weeks. Three of them turned out to be actual explosives. Police found two viable pipe bombs July 21 and one other July 23. The bomb squad safely detonated the devices. It is still unknown who left those bombs in the park or why. Concord police find a handful of unexploded bombs in public places each year, but it is rare for them to find so many in a single place. Source: http://www.mercurynews.com/breaking-news/ci_15696026

Communications Sector

FCC seeks public comment on creation of cybersecurity plan. The Federal Communications Commission released a notice earlier the week of August 9 requesting public comment on the creation of an anticipated FCC plan that looks to address cybersecurity. The plan, the Cybersecurity Roadmap, seeks to identify vulnerabilities to core Internet protocols and develop solutions in response to cyber threats and attacks. The Cybersecurity Roadmap was recommended as an initial step forward in the area of cybersecurity as part of the Commission's National Broadband Plan. Specifically, the NBP recommended the FCC issue, in coordination with the Executive Branch, a plan to address cybersecurity. FCC looks to finalize the Cybersecurity Roadmap by November 2010. "Cybersecurity is a vital topic for the commission because end-user lack of trust in online experiences will quell demand for broadband services, and unchecked vulnerabilities in the communications infrastructure could threaten life, safety and privacy," FCC stated. Source:

http://www.executivegov.com/2010/08/fcc-seeks-public-comment-on-creation-of-cybersecurity-plan/

Germany bans BlackBerrys and iPhones on snooping fears. The German government has advised ministers not to use BlackBerry and iPhone devices due to "a dramatic increase of attacks against" its networks. A general ban on the use of smartphones in certain German ministries is also being considered, the Federal Interior Minister confirmed August 9 to the country's business daily newspaper Handelsblatt. He said that ministers and senior civil servants had been told to instead use Simko2 gadgets offered by T-Systems, following advice from the German federal office for information security (BSI). Berlin expressed concern that data for the BlackBerry smartphone passes through two Research in Motion centers in the UK and Canada. He added that there was a possible risk of "political IT attacks" from organized crime and foreign intelligence agencies and said that such harm to the government could increase with the use of the BlackBerry and other smartphones. His comments came after Canada-based RIM was forced to shift servers to Saudi Arabia after that country briefly banned use of the BlackBerry. Government officials in the United Arab Emirates also threatened to restrict the BlackBerry service. Source: http://www.theregister.co.uk/2010/08/10/german_government_mulls_blackberry_iphone_ban/

4chan users seize Internet's power for mass disruptions. Corporations spend millions of dollars trying to understand and control traffic on the Internet, and more often than not they don't succeed. 4chan has mastered the feat for free. Created seven years ago by a 15-year-old, 4chan is a vast web of anonymous, uncensored message boards. No one is in charge, but the site's users have managed to pull off some of the highest-profile collective actions in the history of the Internet. The June 17 takeover of Google Trends, the powerful tool that companies use to track what's hot on the Internet, was not the first time 4chan succeeded in outwitting Google. The site's users have also managed to get a swastika, symbols depicting planes crashing into the World Trade Center and the words "[expletive] you google" on the trends list. Trying to game Google to make a search popular is not illegal, but some of the other pranks have brought inquiries by the Securities and Exchange Commission, the Department of Homeland Security and the FBI. Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/08/09/AR2010080906102.html

(North Carolina) **Copper thieves hit cell tower.** Police suspect theives broke into the cell phone tower complex at 1319 Second Street SE behind Peoples Bank sometime between 8 a.m. and 1:30 p.m. August 4. Once inside the 8-foot high barbed wire-topped fence, they cut copper wires from the base of the tower and the amplifier at the base of the tower. Copper bars from at least three batteries were stolen as well. The tower is operated by AT&T and Sprint. The stolen copper was worth $4,500, according to the police report. The site attendant reported the theft when he arrived at the site and found the four locks on the gate were unlocked and the gate was open. The Hickory Police Department is investigating the theft. Source: http://www2.hickoryrecord.com/content/2010/aug/06/copper-thieves-hit-cell-tower/news/

Google and Verizon offer a vision for managing Internet traffic. Google and Verizon on August 9 introduced a proposal for how Internet service should be regulated — and were immediately criticized by groups that favor keeping the network as open as possible. According to the proposal, Internet service providers would not be able to block producers of online content or offer them a paid "fast lane." It says the Federal Communications Commission should have the authority to stop or

fine any rule-breakers. The proposal, however, carves out exceptions for Internet access over cellphone networks, and for potential new services that broadband providers could offer. In a joint blog post, the companies said these could include things like health care monitoring, "advanced educational services, or new entertainment and gaming options." The two companies are hoping to influence regulators and lawmakers in the debate over a principle known as net neutrality, which holds that Internet users should have equal access to all types of information online. But some proponents of net neutrality say that by excluding wireless and other online services, Google and Verizon are creating a loophole that could allow carriers to circumvent regulation meant to ensure openness. Source: http://www.nytimes.com/2010/08/10/technology/10net.html?src=busln

Critical Manufacturing

Toyota brakes not used in 35 of 58 accidents probed, U.S. says. Drivers of Toyota vehicles failed to apply the brakes in 35 of 58 crashes tied to unintended acceleration, U.S. regulators said in a report bolstering the automaker. The National Highway Traffic Safety Administration also saw no evidence of electronics-related causes for the accidents in reviewing the vehicle recorders, known as black boxes, the agency said yesterday in the interim report to lawmakers. Toyota has said there is no evidence of flaws in electronic controls on its vehicles and that motorists in some cases confused the accelerator and brake pedals. The company, the world's largest automaker, has recalled more than 8 million vehicles worldwide in the past year for defects such as pedals that stuck or snagged on floor mats. " NHTSA officials have drawn no conclusions about additional causes of unintended acceleration in Toyotas beyond the two defects already known — pedal entrapment and sticking gas pedals," the agency said in the report provided for a briefing to lawmakers in Washington. Toyota has examined more than 4,000 vehicles and hasn't found its electronic throttle controls to be a cause of unintended acceleration in them, a spokesman said. Source: http://www.bloomberg.com/news/2010-08-10/toyota-brakes-not-used-in-35-of-58-accidents-probed-u-s-says.html

Honda recalling Accords, Civics, Elements over ignition flap. Honda Motor Co. Ltd. is recalling about 383,000 Accord, Civic and Element vehicles in the U.S. after receiving several complaints of a potentially dangerous malfunction with the ignition interlock feature that has caused at least one minor injury. The automaker said August 9 that the recall applies to 117,000 Civics and 197,000 Accords, all model-year 2003. Honda also is recalling about 69,000 Element vehicles with 2003 and 2004 model years. The company said the vehicles' ignition interlock mechanism can become worn or damaged over time and eventually allow the key to be removed when the vehicle isn't in park. Such a malfunction could cause the vehicle to roll away and potentially cause a crash. Several incidents, including one that included a minor injury, have been reported. Source: http://columbus.bizjournals.com/columbus/stories/2010/08/09/daily5.html

Defense/ Industry Base Sector

Ex-B-2 engineer guilty of helping China develop stealth cruise missile. A former B-2 stealth bomber engineer has been convicted of helping China develop a cruise missile that can evade heat-seeking, air-to-air missiles. Prosecutors said he sold the classified technology to pay for his luxury home in Hawaii. A federal jury in Honolulu convicted the engineer on 14 of 17 counts of selling classified materials, money laundering and tax evasion. He was also charged with attempting to sell classified

stealth technology to the Swiss government and businesses in Israel and Germany. Jurors acquitted him of three minor espionage charges, the Honolulu Star-Advertiser says. Prosecutors said the 66-year-old, who helped develop the propulsion system for the B-2 when he worked for Northrop from 1968 to 1986, designed the exhaust nozzle for the cruise missile so he could pay the $15,000-a-month mortgage on a luxury home. Source: http://content.usatoday.com/communities/ondeadline/post/2010/08/ex-b-2-engineer-guilty-of-helping-china-develop-stealth-cruise-missile/1

Senators are worried about counterfeit Defense supplies. The Defense Department's supply chain is vulnerable to the infiltration of counterfeit parts, potentially jeopardizing the lives of American soldiers, according to two Democratic senators. In an August 6 letter to the undersecretary of Defense for acquisition, technology and logistics, the Senators argued the Pentagon was not doing enough to protect the system from imitation supplies, many of which originate overseas. "Counterfeit parts manufactured offshore not only hurt American manufacturing and competitiveness, but in this case, have the potential to put our military at risk and jeopardize our national security missions," one said. The letter cited two recent reports that detailed serious weaknesses in Defense's ability to root out fake supplies. In January, the Commerce Department's Bureau of Industry and Security found all elements of the Defense and international supply chain have been directly affected by counterfeit electronics. The assessment, which covered 2005 to 2008, focused on discrete electronic components, microcircuits and circuit board products. A total of 387 companies and organizations, representing all five segments of the supply chain participated in the study. Investigators found 39 percent of companies and organizations encountered counterfeit electronics during the four-year period. The number of incidents grew from 3,868 in 2005 to 9,356 in 2008, the report said. Source: http://www.govexec.com/dailyfed/0810/080910rb1.htm

(Utah) **HAFB criticized again over handling of nuke-related items.** Hill Air Force Base is again facing criticism for the way it handles — or mishandles — materials used to arm, launch or release nuclear weapons. This time, inspectors say the base failed to account for more than 100 nuclear-related parts in recent inventories — which could lead to undetected theft. The Air Force censored which items had been missed, but the unit involved handles nuclear missile maintenance. Inspectors also said that when Hill officials found discrepancies in inventory data, they simply changed codes on forms without verifying actual conditions. And the inspectors said some nuclear-weapons related items were stored in containers marked with codes for other parts, which could lead to shipping the wrong item. That is according to Air Force Audit Agency reports written in January but just recently obtained by the Deseret News through a Freedom of Information Act request. Source: http://www.deseretnews.com/article/700054456/HAFB-criticized-again-over-handling-of-nuke-related-items.html

Emergency Services

Social media emerge as digital avenue for emergency response. Many people are now using Facebook postings and Twitter to report emergencies or call for help — and they expect government response agencies to be paying attention, according to a new survey. The American Red Cross' "Social Media and Disasters and Emergencies" survey of 1,058 adults indicates that 18 percent would turn to digital social media if calls to 911 were unsuccessful. Sixty nine percent of the adults surveyed said emergency response agencies should regularly monitor their Web sites and social media networks so

they can respond promptly to requests for help posted there; 74 percent said they would expect help to arrive in an hour. Fifty-two percent said they would send a text message to an agency on behalf of someone they knew who needed help. If the Web users knew someone who needed emergency help, 44 percent said they would ask other people in their social network to contact appropriate authorities; 35 percent would post a request for help directly on a response agency's Facebook page and 28 percent would send a direct Twitter message to responders. Red Cross officials said the survey illustrates that the public is using social media for emergencies and public agencies need to be ready to respond. Source: http://fcw.com/articles/2010/08/12/social-media-emerging-as-digital-avenue-for-emergency-response.aspx

(Virginia) **Suspicious package prompts Hampton police evacuation.** A suspicious package was examined and cleared this morning after someone found it outside police headquarters August 9 night on Lincoln Street in Hampton, Virginia. The package was found and police were alerted just before 11 p.m., said a police spokeswoman. The building was evacuated and several streets around the building were closed while the bomb squad from Newport News checked the package, the spokeswoman said. Authorities said the area was safe about 1 a.m. August 10, the spokeswoman said. She did not know what was inside the package. Source: http://hamptonroads.com/2010/08/suspicious-package-prompts-hampton-police-evacuation

Energy

(Missouri) **Suspected pipe bomb explodes at Lake Saint Louis electric substation.** Lake Saint Louis Police said an apparent pipe bomb exploded about 3 a.m. August 12 at a Lake Saint Louis electric substation and caused minor damage to an electric substation operated by Cuivre River Electric Cooperative. Police are investigating whether the suspected pipe bomb explosion is connected to several gasoline-filled milk jugs found at the same substation last July. Police said an alarm drew a police officer to the substation. The officer saw what he thought were sparks, so he returned to his vehicle and was pulling forward as the device exploded behind him. Officers searched the area after the explosion but did not find anyone. Remnants of the exploded device were found atop a control box. A chain-link fence surrounding the Woodland Marina substation had been cut. The explosion did not cause power outages in the area. Last year's case was never solved. Agents with the Bureau of Alcohol, Tobacco, Firearms and Explosives are investigating both incidents. Source: http://www.stltoday.com/news/local/stcharles/article_53a4211f-e254-5268-9ebc-8fcd59201e85.html

Huge ice island could pose threat to oil, shipping. An island of ice more than four times the size of Manhattan is drifting across the Arctic Ocean after breaking off from a glacier in Greenland. Researchers are in a scramble to plot the trajectory of the floating ice shelf, which is moving toward the Nares Strait separating Greenland's northwestern coast and Canada's Ellsemere Island. If it makes it into the strait before the winter freeze, it would likely be carried south by ocean currents, hugging Canada's east coast until it enters waters busy with oil activities and shipping off Newfoundland. Although it is likely to break up as it bumps into other icebergs and jagged islands, the chunks of ice could be large enough to threaten Canada's offshore platforms in the Grand Banks off Newfoundland. The Canadian Ice Service estimates the journey will take one to two years. While Greenland's glaciers break off thousands of icebergs into Arctic waters every year, scientists say this ice island is the

biggest in the northern hemisphere since 1962. Source: http://www.google.com/hostednews/ap/article/ALeqM5i1V_CpYIC18MffBDIB6mjBCwuagQD9HGS2C80

Stuxnet could hijack power plants, refineries. The Stuxnet worm, which made headlines in July, can conceivably interfere with critical operations of a plant to do things like close valves and shut off output systems. It is written to steal code and design projects from databases inside systems found to be running Siemens Simatic WinCC software used to control systems such as industrial manufacturing and utilities. It can remotely download files, execute processes, delete files. The Stuxnet software also has been found to upload its own encrypted code to the Programmable Logic Controllers (PLCs) that control the automation of industrial processes and which are accessed by Windows PCs. "... At an energy production plant, the attacker would be able to download the plans for how the physical machinery in the plant is operated and analyze them to see how they want to change how the plant operates, and then they could inject their own code into the machinery to change how it works," a Symantec researcher said August 12. The Stuxnet worm propagates by exploiting a hole in all versions of Windows in the code that processes shortcut files ending in ".lnk." It infects machines via USB drives but can also be embedded in a Web site, remote network share, or Microsoft Word document, Microsoft said. Microsoft issued an emergency patch for the Windows Shortcut hole last week, but just installing the patch is not enough to protect systems running the Siemens program because the malware is capable of hiding code in the system that could allow a remote attacker to interfere with plant operations without anyone at the company knowing. Source: http://news.cnet.com/8301-27080_3-20013545-245.html

The flow has slowed through the trans-Alaska oil pipeline. The flow has slowed through the trans-Alaska oil pipeline and it is likely to keep declining over the next decade, possibly causing dangerous ice and corrosion problems and hampering delivery of North Slope oil to the rest of the U.S. The pipeline is carrying only about 660,000 barrels of oil a day, and production from the North Slope's aging fields is set to steadily decline over the next decade. Engineers have warned that the pipeline — the only means of delivery of North Slope oil — will develop potentially dangerous problems with corrosion and ice if flows drop below 500,000 barrels a day, as they are expected to within the next five to 10 years. A study to be completed in December will determine just how low the oil flow can go before the pipeline is no longer viable. Options include heaters or chemical additives to keep ice from forming, lowering the water content of the oil before pumping or redesigning the "pigs" that course through the pipeline and clean it of wax buildup. Another is to just give up and build a smaller-diameter pipe. Source: http://articles.latimes.com/2010/aug/10/nation/la-na-alaska-oil-20100810

U.S. electricity blackouts skyrocketing. Experts on the nation's electricity system point to a frighteningly steep increase in non-disaster-related outages affecting at least 50,000 consumers. During the past two decades, such blackouts have increased 124 percent, up from 41 blackouts between 1991 and 1995, to 92 between 2001 and 2005, according to research at the University of Minnesota. In the most recently analyzed data available, utilities reported 36 such outages in 2006 alone. "It's hard to imagine how anyone could believe that, in the United States, we should learn to cope with blackouts," said a University of Minnesota professor, a leading expert on the U.S. electricity grid. He supports construction of a nationwide "smart grid" that would avert blackouts and save billions of dollars in wasted electricity. A smart grid is an automated electricity system that improves the reliability, security and efficiency of electric power. It more easily connects with new energy

sources, such as wind and solar, and is designed to charge electric vehicles and control home appliances via a so-called "smart" devices. Source: http://www.cnn.com/2010/TECH/innovation/08/09/smart.grid/index.html?hpt=C1

Food and Agriculture

CDC lists top food pathogens. Surveillance data on foodborne disease outbreaks in 2007 revealed that norovirus and Salmonella contamination were the leading causes, with poultry, beef, and leafy greens the most common foods involved, the CDC reported in the August 13 issue of Morbidity and Mortality Weekly Report. The analysis also indicated that no cause was ever found for about one-third of outbreaks and a quarter of the victims. Nearly 1,100 outbreaks involving 21,244 individual illnesses were covered by the data, supplied by public health laboratories in all 50 states, the District of Columbia, and Puerto Rico. The CDC researchers noted that these were just a handful of the estimated 76 million illnesses occurring in the U.S. annually from contaminated food. Of the 734 outbreaks with known etiologies in 2007, 320 involved bacterial pathogens, 324 were traced to viruses, 49 involved chemical contamination (mostly of microbial origin), and five were parasitic infections. Another 36 had more than one cause. All but seven of the viral outbreaks stemmed from norovirus, which gets into food products when infected workers fail to wash their hands. Salmonella accounted for 142 of the bacterial outbreaks in 2007, including two of the three largest, the CDC researchers reported. Those outbreaks included 802 illnesses traced to tainted hummus and 401 illnesses from frozen pot pies. Rodents in food packaging and distribution facilities are the most common source of Salmonella contamination. Source: http://www.medpagetoday.com/PublicHealthPolicy/PublicHealth/21653

(Vermont) **Popular tour shuttered over terrorism concerns.** Maple syrup wholesaler Maple Grove Farms in St. Johnsbury, Vermont shuttered a factory tour as a result of "food-defense" concerns that have sprouted since the September 11th attacks. The federal government has not instituted a blanket prohibition on factory tours. But post-9/11 guidelines developed by DHS and FDA have shaped the voluntary food-safety standards that companies like Maple Grove must meet in order to sell their wares to major retailers. Those retailers, the general manager at Maple Grove Farms says, require a "Safety Quality Food" certification. The director of business operations for Safe Quality Food — the entity that created the standards — says two "food-defense" guidelines added since the September 11th attacks have affected factory tours. "The first is being able to restrict certain personnel to their production area, and the other is regarding a facilities' ability to manage the coming and going of visitors to the facility," he says. The Maple Grove manager says retrofitting the building to satisfy the standard would be too costly. Ben & Jerry's must also adhere to strict food-safety standards, maintains sufficient distance between visitors and production lines at its Waterbury factory, according to a spokesperson there. The director emeritus of the National Center for Food Protection and Defense says his organization has conceived "a number of scenarios that would be absolutely catastrophic if certain select agents or toxins were introduced at vulnerable points during the food production supply chain." Source: http://www.rutlandherald.com/article/20100812/NEWS03/708129930/-1/RSS10

Fresh Express recalling some salad products. Fresh Express, of Salinas, California, on August 10 voluntarily recalled 2,825 cases of its Veggie Lovers Salad because of a possible health risk from Listeria monocytogenes. The recalled salad mix has a product code of I208 and use-by date of August

10. The salad is being pulled from shelves after one package tested positive for the bacterium in a sample test conducted by the Ohio Department of Agriculture. No illnesses have been reported, the U.S. Food and Drug Administration said. The salad mix was distributed to 13 states with the potential for redistribution by customers to additional states. According to the FDA and Fresh Express, the product was distributed to Missouri, Michigan, Ohio, Illinois, Wisconsin, Indiana, Maryland, Massachusetts, New York, Kansas, Kentucky, Pennsylvania and New Jersey. The mix could then have been sent to Arkansas, Tennessee, West Virginia, Iowa, Minnesota, Virginia, Vermont, New Hampshire, Nebraska, Rhode Island, Pennsylvania, Mississippi and the District of Columbia. Source: http://www.google.com/hostednews/ap/article/ALeqM5g7TGZ9XERdDzj8NJi2hRTuRIxqUAD9HHOAL80

Disease that rots shells threatens Northeast lobster industry. A disease that rots the shells of lobsters is threatening the Northeast's $20-million lobster industry, scientists said August 11. The disease, decimating lobsters since the mid-1990s, could mean new regulations for fishermen already struggling with a bad economy, said the deputy chief of the state Department of Environmental Management's Division of Fish and Wildlife. "Shell disease escalated in 1997, exploded rapidly, and shows no signs of abating," he said. The disease affects about 30 percent of New England's lobster population. Rhode Island fishermen have been hard hit. In 1999, the lobster industry generated $30 million and employed 425 fishermen. Four years later, the industry produced $16.7 million and employed 279. Those numbers continue to fall. The disease's cause and how it spreads remain a mystery. Epizootic shell disease was first noticed decades ago, when fishermen observed small black spots on lobster shells. The disease does not taint the meat of the lobsters. But it discolors and erodes the shells, making them less marketable. In extreme cases the shells rot away and the weakened lobsters are killed by secondary infection or other threats. Egg-carrying females are most susceptible to the disease. New bacteria might be the culprit, said some scientists. Source: http://www.projo.com/news/content/LOBSTER_SHELL_DISEASE_08-12-10_8IJHABL_v9.2535284.html

(California) **Moth prompts countywide quarantine.** North County, California, growers will face limited restrictions under a countywide agricultural quarantine proposed to stop the spread of potentially destructive light brown apple moths ---- six of which were captured July 30 near Balboa Park in San Diego, officials said August 10. Restrictions placed on North County growers were expected to be less costly and time-consuming than those imposed under the Mediterranean fruit fly quarantines in Fallbrook and Escondido, officials said. Officials said most growers would need only to register their farms with authorities, and submit to placement and inspection of traps on their properties. Growers of nursery crops such as cut flowers would also have to submit to a one-time inspection of their properties, the county agriculture commissioner said. Plant nurseries, which represent about $1 billion of San Diego County's $1.5 billion agricultural industry, are most at risk. Source: http://www.nctimes.com/news/local/sdcounty/article_df4c7dfc-4ea6-5120-ac11-d91ee774c924.html

USDA plans to require ID for interstate livestock. Federal officials looking to head off livestock disease outbreaks are drafting regulations that would require farmers to identify animals that move across state lines. The aim is to reduce illness and deaths by making it easier for officials to trace brucellosis, tuberculosis and other diseases to a particular group of animals, location and time. The regulations are being drafted six months after the U.S. Department of Agriculture dropped an

unpopular voluntary program meant to trace livestock movement, and they are expected to be implemented in 2013. "A voluntary system has not worked so far, and that's why the USDA has gone back to the drawing board and created a system that relies much more strongly on compulsory or mandatory identification instead of voluntary," said the Montana state veterinarian and a member of the USDA working group drafting the new rule. Last year, more than 19 million of the nation's 30 million beef cows and 9 million dairy cows crossed state lines. Source: http://www.usatoday.com/news/washington/2010-08-08-livestock-usda-regulations_N.htm?csp=34news

Salmonella outbreak tied to Mexican fast-food chain. State health authorities suspect lettuce and tomatoes served at Taco Bell restaurants may have caused a salmonella outbreak that sickened dozens of people from Kentucky to Oregon. The charges are counter to what federal food safety authorities have been reporting. According to media reports, rare types of salmonella caused illnesses in more than 150 people who dined at Irvine, Calif.-based Taco Bell Corp.'s locations in Ohio, Kentucky, Indiana, Wisconsin and Oregon during late June, when illnesses peaked. Centers for Disease Control investigators, however, are not blaming lettuce or tomatoes and have not warned diners against eating certain foods or dining at particular restaurants. "The extensive traceback effort was initiated to determine if a common source or supplier could be identified to help focus the epidemiologic investigations. No common food source was identified in either traceback," the agency stated in an Aug. 4 news release. In reports in the Louisville Courier and the Portland Oregonian, a senior epidemiologist with Oregon's public health department said scientists suspect lettuce and tomatoes singularly or together. The CDC did not name the restaurant, but said its analysis indicated the sicknesses after eating at a Mexican-style fast food restaurant chain. Source: http://thepacker.com/UPDATED--Salmonella-outbreak-tied-to-Mexican-fast-food-chain/Article.aspx?oid=1201747&fid=PACKER-TOP-STORIES&aid=657

(Michigan; Illinois) **Scientists: Carp may have been planted near lake.** A 3-foot-long Asian carp discovered in a Chicago waterway near Lake Michigan appears to have spent most of its life there and may have been planted by humans who did not know what type of fish it was or the environmental risk it posed, researchers said August 5. Tests of chemical markers in the bighead carp suggest it was not a recent arrival to the waterway and probably did not get there by evading an electric barrier meant to prevent the species from infesting the Great Lakes, said a fisheries biologist at Southern Illinois University Carbondale. He acknowledged the findings were not certain because of incomplete data and were based on a number of assumptions. The 20-pound bighead was netted June 22 in Lake Calumet on Chicago's South Side, about six miles from Lake Michigan. It was the first Asian carp seen above the barrier, although scientists have reported numerous findings of their DNA in waterways between the barrier and Lake Michigan. Source: http://www.detnews.com/article/20100805/METRO/8050455/1409/metro

Tainted pet food behind human salmonella outbreak—study. Tainted pet food may be the reason behind human salmonella outbreak, findings of a new U.S. research suggests. According to the study, dry pet food and cross-contamination after feeding a pet in the kitchen is responsible for salmonellosis outbreak in 21 eastern U.S. states between 2006 and 2008. The outbreak sickened 79 people, with almost 48 percent of the cases occurring among children under age 2, according to CDC veterinary epidemiologist and study's coauthor. As the salmonella can transmit from pet food to humans easily, the epidemiologist said, "Children don't have to put pet foods in their mouths to

become ill." No known cases of human salmonella linked with wet pet food have been reported, investigators highlighted. Source: http://www.themoneytimes.com/featured/20100809/tainted-pet-food-behind-human-salmonella-outbreakstudy-id-10123754.html

Government Sector (including Schools and Universities)

(Georgia) **Driver crashes into jail, says she has explosives.** A woman crashed her car into the front of the Gordon County Sheriff's office Thursday morning, officials said, but this crash was no accident — the woman threatened officers by alleging she had a bomb. The suspect, 24, attempted to drive her blue 2005 Toyota Corolla through the front entrance of the building, which also houses the jail, a Georgia Bureau of Investigations spokesman said. A statue memorializing fallen soldiers obstructed her path, causing the vehicle to stop. "Had that memorial not been there, she would've gone right through the door," the suspect told the AJC. The vehicle was headed toward the front entrance of the sheriff's office, not the front entrance to the jail, a news release said. There were several staff members and visitors inside the front entrance, but no one was injured. As Gordon County deputies evacuated the building, the suspect began threatening she had an explosive device in her vehicle. Gordon County called in GBI agents, Federal Bureau of Investigation agents and Georgia State Patrol officers to assess her threat. After taking her into custody, the GBI used a robot to inspect her vehicle for an explosive device, but found no bomb. The suspect sustained "minor injuries" and was transported to Gordon Hospital where she is under guard. Source: http://www.ajc.com/news/driver-crashes-into-jail-590731.html

(Kentucky) **Rocket leaking nerve-gas vapor at Blue Grass Army Depot is contained.** A rocket leaking nerve-gas vapor was placed into a leakproof container August 11, officials at Blue Grass Army Depot in Madison County said. On August 10, toxic chemical crews found the M55 rocket leaking vapor within its shipping and firing tube. In the so-called "overpack" process, the rocket, still in its shipping and firing tube, was placed in a large container designed to hold leaking rockets. The rocket was then moved to another igloo which holds only overpacked munitions. The leak posed no danger to Madison County residents, Army officials said. Both county and state emergency-management agencies were notified of the leak. Source: http://www.kentucky.com/2010/08/11/1388509/rocket-leaking-nerve-gas-vapor.html#ixzz0wUUMUPSR

(District of Columbia) **EEOB evacuated briefly due to suspicious package.** Numerous reports on Twitter, and word from DC Fire & EMS, show that the Eisenhower Executive Office Building on 17th Street just south of Pennsylvania Ave NW is being evaucated due to a suspicious package referred to by DC Fire & EMS as "haz mat unknown substance," on the morning of August 11. The All-clear was given just after 8:20 this morning. This is the third suspicious package in a prominent location in as many days, with suspicious packages shutting down 13th & New York Avenue on Tuesday and K & I streets between 7th & 9th streets on August 9. Source: http://www.welovedc.com/2010/08/11/eeob-evacuated-briefly-due-to-suspicious-package/

(Guam) **Guam air base steps up security after bomb threat.** A suspect is in custody following a bomb threat at Guam's Andersen Air Force Base. The Air Force says the base stepped up security around 12:30 p.m. Thursday, but had returned to normal operations by 3 p.m. Explosive ordnance disposal experts investigated the threat before the all-clear was sounded. The Air Force says the response

allowed base officials to isolate the incident and get the base back to normal status quickly. No other information on the incident was immediately available. Source: http://www.google.com/hostednews/ap/article/ALeqM5hykMCQdNkVzuwsuFmnp6gZ9XDw9gD9HHU0681

(Oklahoma) **Suspicious fire destroys building at Deep Fork wildlife refuge near Okmulgee.** Federal investigators are looking into a suspicious fire that destroyed the initial construction work on a new office building at the Deep Fork National Wildlife Refuge near Okmulgee. Officials say construction for the building, which was about 35 percent complete, began in June and was scheduled to be open to the public early next year. It is not clear yet if it is an arson case, but a reward is being offered for information in connection with the fire. The U.S. Fish and Wildlife Service, in cooperation with the FBI, ATF, local fire department and other law enforcement agencies are cooperating in the investigation. Source: http://www.newson6.com/Global/story.asp?S=12954824

Agencies could be prone to new kind of sophisticated cyberattack. Federal computer networks are vulnerable to the same type of sophisticated cyberattack that recently cost a global bank more than $1 million in a month, according to a security company official. Hackers used a "man-in-the-browser" attack to steal a total of $1,077,000 from about 3,000 customers of a large financial institution between July and August, a report released by M86 Security on Tuesday indicated. In such attacks, the perpetrator installs on the victim's computer Trojan horse software capable of modifying Web transactions in real time. The report did not name the bank because an investigation is currently under way, but said the victims were located primarily in the United Kingdom. While big payouts often are the motivation for man-in-the-browser attacks, hackers could use a similar strategy to steal classified or other sensitive information from federal agencies, said the vice president of technology strategy for M86 Security. "Any websites that [enable] large financial transactions or [the exchange] of sensitive information, of which government has quite of a few, are at risk of this type of cyberattack," he said. He noted advanced security controls, including multifactor authentication, won't protect systems from man-in-the-browser attacks, because the software running on infected machines "looks over the shoulders" of users who have the appropriate credentials. Source: http://www.nextgov.com/nextgov/ng_20100810_7392.php

(Oklahoma) **Suspicious package found near capitol.** Oklahoma City police called in their bomb squad after a driver noticed a suspicious package with wires in the road near the Capitol early Wednesday morning. The bomb squad blocked off the area near 21st Street and Lincoln Boulevard from midnight until 2 a.m. while they investigated. Using a robot, the bomb squad was able to determine that the suspicious device was a piece of a water heater. No one was hurt and the area around the Capitol is back open for the morning commute. Source: http://www.koco.com/r/24589974/detail.html

(California) **Bomb threat causes brief scare at Stanford billing center.** Palo Alto police responded August 6 to a report of a bomb inside the Stanford University billing center, but the threat did not even prompt an evacuation of the building. A Palo Alto police spokesman said officers went to the building at about 10:10 a.m. after learning a caller told a female employee there was a bomb inside the center at 2690 Hanover St. The caller did not say where the bomb was or when it was set to go off. "The person said there was a bomb on site and hung up," the spokesman said. The patient billing and customer service center is directly across the street from Palo Alto Fire Department's Station 2. About a half dozen officers combed the center, as well as an adjacent building, and determined the

threat was not credible by about 11:10 a.m. A false bomb threat prompted the evacuation of City Hall on January 7. In that case, the caller said the bomb was inside the police department and would be detonated within an hour of the call. The spokesman said because the August 6 bomb threat was called through a "trunk line," it will be difficult to trace its origin and conduct a follow-up investigation. Source: http://www.mercurynews.com/breaking-news/ci_15700361?nclick_check=1

Sea lions, dolphins serve as elite Navy defense. Boats with intimidating displays of weapons patrol the waters at the port at Kings Bay Naval Submarine Base in Georgia. But if underwater intruders elude a patrol boat's sophisticated electronic surveillance, something else waits in the depths that Navy officials say cannot be fooled. For five years, 10 California sea lions and four Atlantic bottlenose dolphins have provided underwater security for Ohio-class submarines ported at Kings Bay as part of the Swimmer Interdiction Security System. Dolphins are trained to use their sophisticated sonar to detect unusual underwater activity and report it to their handlers. A dolphin is sent back to the area with a lighted beacon that it releases near the intruder to alert Navy security forces. Sea lions are trained to carry a special cuff in their mouths that they can quickly clamp around an intruder's leg. The intruder is reeled in by base security by a rope attached to the cuff, which can only be removed with a special key. Kings Bay is home to eight $2 billion Ohio-class submarines. Though they are not native to the East Coast, environmental studies show sea lions have no adverse environmental impact at Kings Bay. The one concern before they arrived was how they would interact with manatees, but it appears the two species are indifferent to each other. It takes about 18 months to train the animals in San Diego, where the Navy's marine mammal program is based. Source: http://www.militarytimes.com/news/2010/08/ap_dolphins_080710/

Information Technology and Telecommunications

Fake malicious software removal tool peddles fake AV. A fake Malicious Software Removal Tool using the actual icon of the legitimate software has been spotted by Trend Micro researchers. Even a first glimpse of the scanning alert looks pretty legitimate, but it's the "Software searching" screen which signals that something might be off. A scan of the computer is simulated finding a well-known malware strain that can only be removed buy purchasing the $99.90 anti-virus that is advertised. This approach might fool the inexperienced computer user, but for those who know what warning signs to look for, there are two very obvious ones: the file size is too small (412,672 bytes) and the tool is not digitally signed. Source: http://www.net-security.org/malware_news.php?id=1428

Facebook bug spills name and pic for all 500 million users. A bug in Facebook's login system allows attackers to match unknown email addresses with users' first and last names, even when they've configured their accounts to make that information private. The information leak can be exploited by social-engineering scammers, phishers, or anyone who has ever been curious about the person behind an anonymous email message. If the address belongs to any one of the 500 million active users on Facebook, the social-networking site will return the full name and picture associated with the account. "Facebook users have no control over this, as this works even when you have set all privacy settings properly," a researcher of Secfence Technologies wrote August 11 on the Full-disclosure security listserve. "Harvesting this data is very easy, as it can be easily bypassed by using a bunch of proxies," he said. Exploiting the vulnerability is as easy as entering the email address into the Facebook sign-on page, typing a random password and hitting enter. To streamline the attack, the researcher has written a PHP script that works with large lists of email addresses. At 8 pm August

11 Pacific Time, the exploit no longer worked. Source: http://www.theregister.co.uk/2010/08/11/facebook_name_extraction_bug/

80 million websites could be compromised due to a flaw in Adobe ColdFusion. As many as 80 million websites could easily be compromised due to a flaw in Adobe's ColdFusion programming language. Users of Adobe's ColdFusion programming language are at risk of losing control of their applications and websites, according to penetration testing company ProCheckUp. It said that it was able to access every file from a server running ColdFusion and harvest usernames and passwords. It said that this was completed through a directory traversal and file retrieval flaw found within ColdFusion administrator. A competent attacker would be able to steal files from the server and gain access to secure areas and eventually modify content or shut down the website or application, according to the company. The co-founder of ProCheckUp claimed that a standard web browser was used to carry out the attack and knowledge of the admin password is not needed. Source: http://www.scmagazineuk.com/80-million-websites-could-be-compromised-due-to-a-flaw-in-adobe-coldfusion/article/176750/

China: ISP level Gmail phishing. Recently, there are many reports from Chinese internet users saying that when they try to access their gmail accounts, they are redirected to a url: hxxp://124.117.227.201/web/gmail/ and asked to re-enter their password. On August 11, NTDTV.com disclosed that the url is a phishing page for stealing users' password. It is believed that local ISPs are involved in the phishing activities. The phishing website looks exactly the same with Gmail but the server is from Urumqi. Moreover, some China Unicom users said that even when they have logged in their Gmail account, the ISP would ask them to "re-enter" their password. The source codes show that it is a phishing activity. The NTDTV.com report suggested that users check the login history of their Gmail account and change their password. In addition, they should check their filter setting and see if some of their emails be redirected to other email account. The report also said that the ISPs level phishing is to create insecure feelings among gmail users and in order to get them to stop using Google's service. Source: http://advocacy.globalvoicesonline.org/2010/08/11/china-isp-level-gmail-phishing/

Vulnerabilities in the Palm Pre and Android smartphones detailed that can see credentials stolen and conversations intercepted. Major vulnerabilities in the Palm Pre and Android smartphones have been detected that could allow data to be stolen. Research by MWR Labs has revealed a major flaw in the Palm Pre that would allow conversations to be intercepted, while a flaw in the Android operating system from 2.0 onwards exists in the browser and allows login credentials and cookies to be harvested. A spokesperson demonstrated that sending a Vcard to the Palm Pre allows an attacker to compromise the phone and intercept all audio close to the phone. They said that this is a completely focused attack that targets a specific user. The director at MWR Labs told SC Magazine that this represents industrial espionage and if this was done over a carrier network it would be breaking the law. The Android flaw involved the use of a login page that can be intercepted over a publicly shared wireless network. The spokesperson said that as the phone is configured to save passwords, any user who connects to a rogue WiFi point can have their credentials stolen. Source: http://www.scmagazineuk.com/vulnerabilities-in-the-palm-pre-and-android-smartphones-detailed-that-can-see-credentials-stolen-and-conversations-intercepted/article/176735/

Germany bans BlackBerrys and iPhones on snooping fears. The German government has advised ministers not to use BlackBerry and iPhone devices due to "a dramatic increase of attacks against" its networks. A general ban on the use of smartphones in certain German ministries is also being considered, the federal interior minister confirmed to the country's business daily newspaper Handelsblatt August 9. He said that ministers and senior civil servants had been told to instead use Simko2 gadgets offered by T-Systems, following advice from the German federal office for information security (BSI). Berlin expressed concern that data for the BlackBerry smartphone passes through two Research in Motion centers in the UK and Canada. The interior minister added that there was a possible risk of "political IT attacks" from organized crime and foreign intelligence agencies and said that such harm to the government could increase with the use of the BlackBerry and other smartphones. His comments came after Canada-based RIM was forced to shift servers to Saudi Arabia after that country briefly banned use of the BlackBerry. Source: http://www.theregister.co.uk/2010/08/10/german_government_mulls_blackberry_iphone_ban/

6 million malicious files found in the past 3 months. Malware has reached its highest levels, making the first six months of 2010 the most active half-year ever for total malware production, according to a new McAfee report. At the same time, spam leveled out with only 2.5 percent growth from Q1 2010. Malware continued to soar in Q2 2010, as there were 10 million new pieces cataloged in the first half of this year. Consistent with last quarter, threats on portable storage devices took the lead for the most popular malware, followed by fake anti-virus software and social media specific malware. With approximately 55,000 new pieces of malware that appear everyday, globally AutoRun malware and password-stealing Trojans round out the Top Two malware threats. After reaching its highest point in Q3 2009, with nearly 175 billion messages per day spam rates have hit a plateau. Cybercriminals took advantage of anticipation on and hype of the FIFA World Cup in South Africa, and used various methods to promote scams and search-engine "poisoning." Globally, the most popular types of spam varied from country to country with some interesting findings. For instance, delivery status notifications, or non-delivery receipt spam, were the most popular in United States, Italy, Spain, China, Great Britain, Brazil, Germany and Australia. Source: http://www.net-security.org/malware_news.php?id=1426

Experts uncover flaws in 'private browsing'. Security experts have warned that many claims about the resilience of 'secure browsing' features are overstated, and that private surfing may be anything but. The researchers at Stanford University are due to discuss their findings at the Usenix Security Symposium in Washington. The top four browsers - Internet Explorer, Firefox, Safari and Chrome - suffer from weak security in their secure browsing options, according to the report, and often fail to prevent user history being exposed. The browsers are also inconsistent in the way they deliver private browsing. Firefox and Chrome protect against web attacks, for example, but Safari protects only against local access. Firefox treats elements of its security differently, according to the research, and exposes some detail even in secure mode. All four browsers contain "privacy violations", the report said. Source: http://www.v3.co.uk/v3/news/2267785/secure-browsing-secure

DNS made easy rallies after punishing DDoS attack. DNS Made Easy has restored services following a vicious denial of service that peaked at 50Gbps August 7. The identity of the perpetrators and their motives remain unclear. One possible scenario is that hackers with a grudge against the site hired a botnet to swamp DNS Made Easy with useless traffic. The firm said it experienced 1.5 hours of actual downtime during the attack, which lasted eight hours. Carriers including Level3, GlobalCrossing,

Tinet, Tata, and Deutsche Telekom assisted in blocking the attack, which due to its size flooded network backbones with junk. DNS Made Easy specializes in global IP Anycast enterprise DNS services, so it is not exactly a likely target for internet attacks, especially one of such ferocity. The SANS Institute's Internet Storm Centre is among the many security watchers keen to learn more about the attack. Source: http://www.theregister.co.uk/2010/08/09/dns_service_monster_ddos/

National Monuments and Icons

(Idaho) **Lightning sparks 14 new fires on Boise National Forest.** Idaho firefighters are responding to 14 new lightning-caused fires on the Boise National Forest while monitoring the two-week old Little Beaver wildfire complex. The Little Beaver fire is 16 percent contained but did not grow much August 10 or overnight. The fire remains at an estimated 4,053 acres. The lightning-caused fire started 15 days ago. There are 240 people assigned to the fire, which has an estimated containment date of October 1. Fire managers said the Little Beaver fire has slowed as wetter and cooler weather moved through the area. Thunderstorms dropped about 3/10ths of an inch in the fire area August 10. The Little Beaver fire is actually a complex of fires being managed together. The Little Beaver Fire, Bernard Lake Fire and Bernard Mountain Fire merged August 3. Source: http://www.kval.com/outdoors/news/100452344.html

(New York) **Statue Of Liberty to close for security upgrades.** The Statue of Liberty will be closed for security upgrades starting about a year from now, depriving tourists a chance to visit the crown, base and pedestal for up to 12 months. Visitors to one of New York's most popular attractions will still be able to visit the park surrounding the statue on Liberty Island, but the security upgrade will restrict access to the statue after October 12, 2011, when the statue celebrates its 125th anniversary. The $26 million dollar project will add fire-proof staircases, elevators and exits, said the superintendent of the Statue of Liberty National Monument. The only exit from the top of the 22-story observation deck is one narrow staircase. More than 5 million people visit the landmark every year, with 20,000 tourists a day flocking to the site during the summer. Source: http://kgmi.com/Statue-Of-Liberty-To-Close-For-Security-Upgrades/7873681

(New Jersey) **Wildfire closes national park hiking trails in N.J.** A wildfire burning in Worthington State Forest has forced some hiking trails to close in the Delaware Water Gap National Recreation Area, which adjoins the state forest in New Jersey. The following trails are closed until further notice to ensure public and firefighter safety: Kaiser Trail: The 2-mile trail is closed from the trailhead on Old Mine Road to the Appalachian Trail; Coppermine Trail: The 1.8-mile trail is closed from the trailhead on Old Mine Road to the Appalachian Trail at Camp Road; Appalachian Trail: The trail is closed from the Mohican Outdoor Center south to Holly Spring. Hikers will follow alternate routes along nearby roads. The Appalachian Trail is open from the Dunnfield Creek trailhead north to Holly Spring. National Park Service firefighters from Delaware Water Gap National Recreation Area and Upper Delaware Scenic and Recreational River are assisting the New Jersey Department of Environmental Protection, Division of Parks and Forestry, with the fire suppression effort. Source: http://www.poconorecord.com/apps/pbcs.dll/article?AID=/20100809/NEWS/8090316

(Missouri) **2,400 marijuana plants found in southeast Missouri sweep.** A three-day marijuana eradication effort in southeast Missouri led authorities to nearly 2,400 plants. The Poplar Bluff Daily American Republic reports the recent operation involved nearly 25 officers from the Drug

Enforcement Administration, Missouri State Highway Patrol, SEMO Drug Task Force, U.S. Forest Service and sheriff's offices in Ripley and Butler counties. The operation focused primarily on public lands, including Mark Twain National Forest. One person was arrested for cultivating marijuana; another was arrested on a methamphetamine-related charge. Source: http://www.kansascity.com/2010/08/09/2137756/2400-marijuana-plants-found-in.html

Postal and Shipping

(South Carolina) **SLED: White powder found in letter sent to Sen. Graham.** Agents with the South Carolina Law Enforcement Division are investigating after they said a white powdery substance was found inside a letter sent to a U.S. Senator's office. The letter was found August 11 at the South Carolina Senator's office on south Main Street, FOX Carolina News reported. SLED said it responded at the request of the FBI. Investigators said they do not think the substance in the letter is harmful, but it has been forwarded to a lab run by the South Carolina Department of Health and Environmental Control for testing. Officials said the Senator was not at the office Thursday. Source: http://www.foxcarolina.com/politics/24612700/detail.html

(Alabama) **Madison County woman receives envelope containing white powder.** Early on the afternoon of August 12, a Madison woman called 911 complaining of burns from a powdery substance that came from an envelope she recieved in the mail. The woman lives on Raymond Road, off of Blake Bottom Road. She reached into a mailbox, grabbed a letter, but it apparently had some white powder inside it. She immediately called for help. This was about 1 p.m. Several agencies responded to the woman's home, including the Monrovia Volunteer Fire Department and Madison County Sheriff's Office. The Huntsville Fire Department also responded with its hazardous materials teams. The FBI is also investigating the situation, and the Postmaster General was notified. The woman who handled the letter was treated for minor injuries. She was taken to a local hospital as a precaution. Source: http://www.whnt.com/news/whnt-possible-chemical-in-mailbox,0,6131994.story

(Texas) **Latest letter containing white powder found at Crowley courthouse in downtown Dallas.** A letter containing white powder was found August 10 at the Frank Crowley Courts Building in downtown Dallas, authorities said. A woman in a district clerk's office opened the letter and called 911 about 2 p.m. Three people were evacuated, and no injuries were reported. A hazardous materials crew quickly determined that the substance was not toxic, and the workers were allowed to return to the office. This is the latest in a series of more than a dozen letters containing powder that have been sent to local businesses and religious institutions. Investigators have yet to determine whether the letters originated from one person or multiple sources. Source: http://www.dallasnews.com/sharedcontent/dws/news/localnews/stories/081110dnmetpowder.3ec4878c.htm

(Washington) **Possible bomb found in mailbox.** The Spokane Valley Police Department is investigating at least two sparkler bomb discoveries in the last week, and now a third victim has come forward. For the last 30 years, the resident has lived with her husband in a rural community in the Spokane Valley. Year after year, she has walked down her driveway to check the mail without much excitement, until July 2. "I started to reach for the mail and then I spotted it and of course backed up and thought hmm, this doesn't look good," the resident explains. The device looked like a bomb and

was covered by letters. The resident backed away, immediately went to tell her husband and then called 911. "It was probably about 10 inches long, maybe two inches in diameter, wrapped in black tape," said the resident. According to the Valley homeowner, the Spokane County Sheriff's Office Bomb Squad removed the explosive device. Then this week, more reports of sparkler bombs being discovered in the area alarmed the resident. Investigators would not say if the sparkler bomb found August 9 near Lynden Road and Trent Avenue is connected to the one left outside the Rock Bar and Lounge in the Spokane Valley last week, but they did say the devices can be deadly. Both cases are under investigation. Source: http://www.kxly.com/news/24574178/detail.html

(Texas) **13 white powder letters delivered in DFW area.** The FBI and U.S. Postal Inspectors confirm they are investigating the delivery of more suspicious letters in North Texas. They now say the total number of letters is 13, following the discovery of the newest one in North Dallas late Friday afternoon. The first letters were found on August 5. By 5 p.m. six letters containing white powder had been delivered to locations across the metroplex. By 11 a.m. on August 6 CBS 11 News learned of five additional letters that had been received. By 5 p.m. on the 6th, the total had risen to 13, according to investigators. Four additional letters arrived the morning of August 6th. They were delivered to a company in Arlington, the Raytheon in Garland, another aerospace company in Grand Prairie, a Raytheon plant on the property of Texas Instruments in Dallas, and Rocket Air Supply company on 111th Street in Arlington. Friday afternoon it was learned that two letters were also found at a Raytheon office in the Boston area. There is no word on if all the letters were sent from the same person or location and investigators. While federal officials would not say if the envelopes contained anything besides the white powder, they are investigating if all of the letter deliveries are related, including an additional one found in the mail room of the Israeli Embassy in Washington. Source: http://cbs11tv.com/local/white.powder.suspicious.2.1846680.html

Public Health

(New York) **5 cases of whooping cough reported in Tioga County.** Five cases of pertussis, commonly known as whooping cough, have been reported in Tioga County, according to county health department officials. "They're mostly school-age children," said the supervising public health nurse for the Tioga County Health Department. "They're scattered. There's no cluster." The health department wants to get the word out before the school year begins, so residents can be aware and protect themselves. The situation isn't unusual because children are together at pools and summer camps and can infect one another, the nurse said. "We had an outbreak in 2004 and 2005, and it started at almost the same time. So far, the disease hasn't spread to neighboring Broome County, said a county Public Health Nurse. Health officials remind people to make sure they're up-to-date with recommended vaccines. Source: http://www.pressconnects.com/article/20100811/NEWS01/8110418/5+cases+of+whooping+cough+reported+in+Tioga+County

Experts outline pandemic preparedness, response issues. The 18 leading experts on influenza, public health, and animal health who made up the Task Force on a One-Health Approach to Influenza recently published their recommendations for preparing and responding to an influenza pandemic or other emerging zoonotic diseases by using the recent H1N1 pandemic as a case study. Publishing their findings in the August 10 edition of Emerging Infectious Diseases, a journal of the Centers for Disease Control and Prevention (CDC), the panel urged improving vaccines and enhancing capacity for

vaccine product, expanding and improving surveillance of influenza viruses, improving early detection of flu in humans and animals, developing new tools to interrupt transmission, and applying new developments from the fields of molecular biology. “One of the largest gaps found in preparedness for [the] pandemic â_¦ was the inability of scientists to translate virus detection and characterization into effective vaccines in an efficient and timely manner,” the panel found, adding that “many of these issues similarly limit development of seasonal human and animal influenza vaccines.” Source: http://www.hstoday.us/content/view/14292/149/

Hospital MRSA infection rates plunge 28 percent. Invasive, hospital-onset methicillin-resistant Staphylococcus aureus infections decreased “dramatically and significantly” by 9.4% per year from 2005 to 2008, a Journal of the American Medical Association report says. Additionally, there was a 5.7% decrease per year in the incidence of healthcare-associated or community-onset MRSA infections.This is the first study of its kind to reflect MRSA findings among outpatients who may have acquired their infections in healthcare settings. This translates to a 28% decrease in hospital-onset invasive MRSA infections and about a 17% decrease in invasive healthcare-associated or community-onset infections over the period studied. For the study, JAMA collected lab reports from nine diverse metro areas representing 15 million people. In all measures, the authors wrote, use of prevention strategies shows that the national priority to reduce these infections has been a success, although “more challenges remain. Increasing adherence to existing recommendations and addressing MRSA transmission and prevention beyond inpatient settings” require further effort. The report was published in Tuesday’s edition of JAMA by researchers from the Centers for Disease Control and Prevention, in collaboration with other investigators in nine states: Georgia, Connecticut, Colorado, California, Maryland, Minnesota, New York, Oregon, and Tennessee. Source: http://www.healthleadersmedia.com/content/QUA-254948/Hospital-MRSA-Infection-Rates-Plunge-28

Health official cautious over end of H1N1 pandemic. The Champaign County, Illinois area saw its last new H1N1 flu cases this past spring, but a different flu strain with the typical respiratory symptoms is now circulating, said a Champaign-Urbana Public Health District Administrator. The administrator also cautioned that headlines declaring the H1N1 pandemic to be over - can be misleading, because H1N1 is still circulating in other parts of the world. “H1N1 is still out there. It’s still making people sick. There were quite a few deaths reported in India last week,” she said. World Health Organization Director-General declared the H1N1 pandemic to be over August 10, based on the findings of experts on the WHO Emergency Committee. The world has moved into the post-pandemic period, she said. Source: http://www.news-gazette.com/news/health/health-care/2010-08-11/health-official-cautious-over-end-h1n1-pandemic.html

Gains in bioscience cause terror fears. Rapid advances in bioscience are raising alarms among terrorism experts that amateur scientists will soon be able to gin up deadly pathogens for nefarious uses. Fears of bioterror have been on the rise since the September 11, 2001, attacks, stoking tens of billions of dollars of government spending on defenses, and the White House and Congress continue to push for new measures.The new fear is that scientific advances that enable amateur scientists to carry out once-exotic experiments, such as DNA cloning, could be put to criminal use. Many well-known figures are sounding the alarm over the revolution in biological science, which amounts to a proliferation of know-how—if not the actual pathogens. “Certain areas of biotechnology are getting more accessible to people with malign intent,” said an expert on biological and chemical weapons at

the James Martin Center for Nonproliferation Studies. A geneticist said last month at the first meeting of a presidential commission on bioethics, "If students can order any [genetic sequences] online, somebody could try to make the Ebola virus." Scientists have the ability to manipulate genetic material more quickly and more cheaply all the time. Just as "Moore's Law" describes the accelerating pace of advances in computer science, advances in biology are becoming more potent and accessible every year, experts note. However, many experts caution that, despite scientific advances, it is still exceedingly tough for terrorists to isolate or create, mass produce and deploy deadly bugs. Tens of thousands of Soviet scientists spent decades trying to weaponize pathogens, with mixed results. Though science has advanced greatly since the Cold War, many of the same challenges remain. Source:
http://online.wsj.com/article/SB10001424052748703722804575369394068436132.html

UK doctors: New superbug gene could spread widely. British scientists have found a new gene that allows any bacteria to become a superbug, and are warning that it is widespread in India and could soon appear worldwide. The gene, which can be swapped between different bacteria to make them resistant to most drugs, has so far been identified in 37 people who returned to the U.K. after undergoing surgery in India or Pakistan. The resistant gene has also been detected in Australia, Canada, the U.S., the Netherlands and Sweden. The researchers say since many Americans and Europeans travel to India and Pakistan for elective procedures like cosmetic surgery, it was likely the superbug gene would spread worldwide. It has been seen largely in E. coli bacteria, the most common cause of urinary tract infections, and on DNA structures that can be easily copied and passed onto other types of bacteria. The researchers said the superbug gene appeared to be already circulating widely in India, where the health system is much less likely to identify its presence or have adequate antibiotics to treat patients. Still, the numbers of people who have been identified with the superbug gene remains very small. Experts said while people checking into British hospitals were unlikely to encounter the superbug gene, they should remain vigilant about standard hygiene measures like properly washing their hands.Researchers called for international surveillance of the bacteria, particularly in countries that actively promote medical tourism. Source:
http://www.google.com/hostednews/ap/article/ALeqM5gpFQ3Bz7hIFhSsHlYpROVwTVwwoAD9HHAI6G0

Healthcare suffers more data breaches than financial services so far this year. Healthcare data breaches have swollen in 2010: Identity Theft Resource Center reports show that compromised data stores from healthcare organizations far outstrip other verticals this year. According to figures updated last week, healthcare organizations have disclosed 119 breaches so far this year, more than three times the 39 breaches suffered by the financial services industry. Though many of these breaches aren't necessarily caused directly by unauthorized access or hacking of healthcare databases, some experts believe that the high numbers are due to lax handling of how data is stored and accessed within these databases. This atmosphere, along with the extreme portability of healthcare data due to consumer devices and laptops and increasing numbers of malicious insiders seeking to profit from electronic medical records (EMRs) and other patient data, has formed a poisonous combination within the industry. One of the biggest issues healthcare organizations face in regards to database security is the issue of what happens to data once it gets outside of the database. The patterns behind many of this year's biggest healthcare breaches seem to corroborate experts' worries. Some of the most frequent causes behind breaches in 2010 and in recent memory are lost and stolen laptops as well as back-up tapes, hard drives, and other portable media. Source:

http://www.darkreading.com/database_security/security/attacks/showArticle.jhtml?articleID=226600307

(California) **CDC asks for more whooping cough tests.** The Centers for Disease Control is encouraging California doctors to do more advanced tests to diagnose whooping cough. CDC scientists have collected only seven biological samples of the illness since the state-wide epidemic began this year. Whooping cough, also known as pertussis, is a respiratory illness caused from bacteria. Different strains of bacteria can cause the disease. There have been 2,500 whooping cough cases confirmed so far this year in California. But CDC scientists have bacterial cultures for just seven of those cases. Labs in San Diego typically run tests that only generate a positive or negative result for whooping cough, rather than classifying the strain. Two of the seven samples the CDC is studying are from infants who died earlier this year from whooping cough. The California Department of health has also requested test samples from the San Diego baby that died of the illness last month. Source: http://www.kpbs.org/news/2010/aug/09/cdc-asks-more-whooping-cough-tests/

TRANSPORTATION

FAA computers still vulnerable to cyberattack. Federal Aviation Administration computer systems remain vulnerable to cyber attacks despite improvements at a number of key radar facilities in the past year, according to a new government review. The Department of Transportation's Inspector General said while the FAA has taken steps to install more sophisticated systems to detect cyber intrusions in some air traffic control facilities, most sites have not been upgraded. And there is no timetable yet to complete the project, the IG said.The FAA said that upgrades to critical air traffic control systems have taken precedence over the intrusion detection improvements at a number of facilities. Without the detection abilities, the FAA cannot effectively monitor air traffic control for possible cyber attacks or take action to stop them. The computer systems used to control air traffic are often in the same building as ones used for administrative functions, but they are not connected. Cyber experts repeatedly warn, however, that in some cases software glitches and other gaps can be exploited by hackers to move between computer systems at critical infrastructure facilities. Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2010/08/12/national/w102757D19.DTL&type=politics

Body scanners going unused at Nigeria airports. Body scanners bought for Nigeria's international airports in the wake of a Christmas Day bomb attempt remain unused months later, though officials said August 11 that U.S. air marshals now protect flights coming into the West African nation. The director general of the Nigerian Civil Aviation Authority said that the government still needs to train officers to man the screening devices already in place at Lagos' Murtala Muhammed International Airport and at the international airport in Abuja. The machines have yet to be installed at the international airports in Kano and Port Harcourt, he said. Security officials suggest that body scanners, which create detailed 3-D images of passengers' figures, would have shown the explosives that prosecutors say the terrorist suspect hid inside his underwear. Nigeria's aviation history remains marred with air fatalities and lax security. The U.S. put a six-year ban on direct flights from Murtala Muhammed International Airport in the 1990s over security concerns. Even today, some passengers encounter officials at the airport who try to solicit cash bribes while baggage handlers rifle through luggage for valuables. Source:

http://www.google.com/hostednews/ap/article/ALeqM5jnbAW4xGSPXKbdaSmGwoH_m6vSxwD9HHAPTG0

(Alaska) **Air Guardsmen work to recover victims from Alaska crash site.** Alaska Air National Guard Armen are aiding victims of a plane that crashed near Dillingham, Alaska, August 9. A downed plane reportedly carrying nine passengers was spotted 285 miles southwest of Anchorage, Alaska. Flight service officials in Dillingham contacted the Alaska ANG's 11th Rescue Coordination Center after losing contact with the De Havilland Twin Otter at around 7 p.m., National Guard officials said. Pararescue Airmen from the Alaska ANG's 212th Rescue Squadron arrived on the scene just before noon August 10. They struggled against rough weather and had been expected to arrive around midnight. A Coast Guard C-130 Hercules is providing support overhead and will be available to take victims in need of serious medical treatment to Anchorage once victims are transported to Dillingham, officials said. News reports estimate at least five fatalities. Source: http://www.af.mil/news/story.asp?id=123217176

(District of Columbia; Maryland; Virginia) **Metro warned of subway threat.** The Washington, D.C. Metro has reportedly been warned about a potential threat to the subway system. According to Channel 4, an internal Homeland Security memo says someone traveled to Turkey last July to obtain a U.S. visa to come to Washington to blow up an unspecified Metro station. "The information that we have has a low level of credibility," Metro's Transit Police Deputy Chief told Channel 4. "There is not a lot of information that suggests a time or place where this person is even capable of conducting such a crime." The Department of Homeland Security alerted Metro August 8 about the unconfirmed threat. Source: http://wtop.com/?sid=2023690&nid=30

US FAA orders fixes in Boeing 747s. The U.S. Federal Aviation Administration has proposed mandatory fixes to Boeing 747-400 airliners to ensure that concerns about potentially hazardous takeoffs are addressed, the Wall Street Journal said. The U.S. air-safety regulator, the week of August 2, moved to require certain engine-related wiring changes. According to the agency, the fixes are necessary to avoid potentially dangerous retraction of flaps, or panels that deploy from the wings to provide extra lift during takeoffs. FAA said that the retracting flaps during critical early phases of flight could result in reduced climb performance and consequent collision with terrain and obstacles, the paper said. The regulators directive will cover nearly 100 Boeing 747s flown by U.S. carriers and equipped with engines manufactured by both General Electric and Pratt & Whitney. A Boeing spokeswoman told the paper that the company issued service bulletins earlier this year urging airlines to voluntarily make the modifications, but only the FAA can mandate U.S. carriers to make such fixes. Source: http://www.reuters.com/article/idUSSGE6780AQ20100809

Water and Dams

Nothing Significant to Report

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: Fusion Center (24/7): 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov ; Fax: **701-328-8175**
State Radio: 800-472-2121 Bureau of Criminal Investigation: 701-328-5500 Highway Patrol: 701-328-2455
US Attorney's Office Intel Analyst: 701-297-7400 Bismarck FBI: 701-223-4875 Fargo FBI: 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, **701-328-8168**